Listing and Amendments to the Claims

This listing of claims will replace the claims that were published in the PCT Application:

[001] (Currently amended) ~~Method~~ A method of enciphering/deciphering a message to be exchanged between a sender and a receiver by way of a communication network, the sender and the receiver both being one among a secure device ~~(1)~~ and a defined client device ~~(C_i)~~ in a network of client devices ~~(C_i, C_j)~~, the method comprising the steps of:

- performing operations of asymmetric cryptography by the secure device ~~(1)~~ and by the defined client device ~~(C_i)~~ respectively with the aid of a private key ~~(n_i, d_i)~~ and of a public key ~~(n_i, e_i)~~, the private key being different from the public key, and

- dispatching ~~(62, 81)~~ at least one public data item ~~(n_i, CID_i)~~ from the defined client device ~~(C_i)~~ to the secure device ~~(1)~~,

~~characterized in that it~~ Wherein the method comprises furthermore, during each send/receive of a message enciphered by the secure device, a step of determining the private key ~~(n_i, d_i)~~ corresponding to the public key ~~(n_i, e_i)~~ of the defined client device ~~(C_i)~~, on the basis of a secret master key ~~(MK)~~ stored in the secure device, and the or each public data item ~~(n_i, CID_i)~~ dispatched by the defined client device ~~(C_i)~~.

[002] (Currently amended) ~~Method~~ The method of enciphering/deciphering a message according to Claim 1, ~~characterized in that~~ wherein the step of dispatching ~~(62, 81)~~ the or each public data item comprises a step of dispatching a part ~~(n_i)~~ of the public key, this part of the public key forming a first part of the private key.

[003] (Currently amended) ~~Method~~ The method of enciphering/deciphering a message according to ~~any one of Claims 1 and 2~~ claim 1, ~~characterized in that~~ wherein the step of dispatching ~~(62, 81)~~ the or each public data item comprises a step of dispatching an identifier ~~(CID$_i$)~~ of the client device ~~(C$_i$)~~, and the step of determining the private key comprises a step of calculating a second part ~~(d$_i$)~~ of the private key on the basis of the said dispatched identifier.

[004] (Currently amended) ~~Method~~ The method of enciphering/deciphering a message according to Claim 3, ~~characterized in that~~ wherein the step of determining the private key ~~(n$_i$, d$_i$)~~ corresponding to the public key ~~(n$_i$, e$_i$)~~ of the client device, comprises a step of enciphering ~~(44, 64, 83)~~ the result ~~(ECID$_i$)~~ of a function applied to the identifier ~~(CID$_i$)~~ of the defined client device ~~(C$_i$)~~, by a symmetric algorithm, with the aid of the secret master key ~~(MK)~~.

[005] (Currently amended) ~~Method~~ The method of enciphering/deciphering a message according to Claim 4, ~~characterized in that~~ wherein the step of determining the private key ~~(n$_i$, d$_i$)~~ corresponding to the public key ~~(n$_i$, e$_i$)~~ of the client device, comprises a step of selecting ~~(45, 65, 84)~~ the second part ~~(d$_i$)~~ of the private key, by a deterministic calculation unit ~~(8)~~, on the basis of the result of the said enciphering of the result ~~(ECID$_i$)~~ of a function applied to the identifier ~~(CID$_i$)~~ of the defined client device ~~(C$_i$)~~.

[006] (Currently amended) ~~Method~~ The method of enciphering/deciphering a message according to Claim 5, ~~characterized in that~~ wherein the step of selecting the second part ~~(d$_i$)~~ of the private key, by the deterministic algorithm, is performed by a selection of a number such that:

- this number is less than the result of the said encipherment of the result ~~(ECID$_i$)~~ of a function applied to the identifier ~~(CID$_i$)~~ of the defined client device ~~(C$_i$)~~,

- this number is the closest to the result of the said encipherment of the result ~~(ECID$_i$)~~ of a function applied to the identifier ~~(CID$_i$)~~ of the defined client device ~~(C$_i$)~~, and is prime to a list of prime numbers.

[007] (Currently amended) ~~Method~~ The method of enciphering/deciphering a message according to ~~any one of Claims 3 to 6~~ claim 3, ~~characterized in that~~ wherein it comprises a step of destruction ~~(49, 67, 87)~~ of the identifier ~~(CID$_i$)~~ of the defined client device ~~(C$_i$)~~ and of all the data ~~(p$_i$, q$_i$, d$_i$, ECID$_i$, e$_i$, n$_i$)~~ calculated on the basis of the identifier so as to determine the private key.

[008] (Currently amended) ~~Method~~ The method of enciphering/deciphering a message according to ~~any one of the preceding claims, characterized in that~~ claim 1 wherein the cryptography operations comprise an operation for identifying a message comprising the following steps:

- signature of the message ~~(85)~~, by the secure device ~~(1)~~, with the aid of the private key ~~(n$_i$, d$_i$)~~ determined during the step of determining the private key,

- transmission of the signature of the message and of the message ~~(86)~~ to the client device for verification of this signature, and

- verification of the signature ~~(87)~~ of the message, by the client device, with the aid of the said public key ~~(n$_i$, e$_i$)~~.

[009] (Currently amended) ~~Method~~ The method of enciphering/deciphering a message according to ~~any one of the preceding claims~~ claim 1, ~~characterized in that~~ wherein the cryptography operations comprise an operation for securing a message comprising the following steps:

- encipherment ~~(61)~~ of a message ~~(m)~~, by the client device ~~(C_i)~~, with the aid of the public key ~~(n_i, e_i)~~,

- transmission ~~(62)~~ of the enciphered message to the secure device ~~(1)~~, and

- decipherment ~~(66)~~ of the message enciphered by the secure device ~~(1)~~, with the aid of the private key ~~(n_i, d_i)~~ determined during the step of determining a private key.

[010] (Currently amended) ~~Method~~ The method of enciphering/deciphering a message according to ~~any one of Claims 3 to 9~~ claim 3, ~~characterized in that~~ wherein it comprises a prior phase of personalizing the said defined client device ~~(C_i)~~, which comprises the following steps:

- generation, by the secure device ~~(1)~~, of a unique secret master key ~~(MK)~~ and of an identifier ~~(CID_i)~~ specific to the said defined client device ~~(C_i)~~ and able to identify it,

- calculation of the said public key ~~(n_i, e_i)~~ of the defined client device ~~(C_i)~~ by a calculation module ~~(5)~~ on the basis of the second part ~~(d_i)~~ of the private key.

[011] (Currently amended) ~~Method~~ The method of enciphering/deciphering a message according to Claim 10, in which the personalization phase furthermore comprises the following steps:

- selection ~~(46)~~ of two secret data consisting of two large prime numbers p_i, q_i, such that $(p_i-1) \times (q_i-1)$ is prime to the second part ~~(d_i)~~ of the private key of the defined client device ~~(C_i)~~, and

- calculation ~~(48)~~ of a modulus n_i of the defined client device ~~(C_i)~~ such that:
  $n_i = p_i \times q_i$, and

- calculation ~~(48)~~ of a part ~~(e_i)~~ of the public key by an extended Euclid algorithm on the basis of the or of each secret data item p_i, q_i and of the modulus n_i of the defined client device ~~(C_i)~~.

[012] (Currently amended) ~~Secure~~ A secure device ~~(1)~~ able to exchange a message with a defined client device ~~(C_i)~~ of a network of client devices ~~(C_i, C_j)~~, over a communication network, the secure device being able to receive at least one public data item ~~(CID_i, n_i)~~ specific to the said defined client device ~~(C_i)~~ and dispatched by the latter prior to any exchange of messages, the secure device ~~(1)~~ comprising:

- means for performing operations of asymmetric cryptography with the aid of a private key ~~(n_i, d_i)~~ corresponding to a public key ~~(n_i, e_i)~~ stored in the defined client device ~~(C_i)~~

~~characterized in that~~ wherein it comprises, furthermore:

- secure means of storage ~~(3)~~ of a master key ~~(MK)~~,

- means ~~(4)~~ of determination of the said private key ~~(d_i, n_i)~~ on the basis of the master key ~~(MK)~~ and of the or of each public data item ~~(CID_i, n_i)~~ dispatched.

[013] (Currently amended) ~~Secure~~ The secure device according to Claim 12, ~~characterized in that~~ wherein the public data item ~~(CID_i, n_i)~~ comprises a part ~~(n_i)~~ of the public key of the said defined client device ~~(C_i)~~ and/or an identifier ~~(CID_i)~~ of the defined client device.

[014] (Currently amended) ~~Secure~~ The secure device according to Claim 13, ~~characterized in that~~ wherein the private key is a mixed key comprising a first part ~~(n_i)~~ corresponding to a part of the public key ~~(n_i, e_i)~~ of the said defined client device ~~(C_i)~~ and a second secret part ~~(d_i)~~ calculated on the basis of the master key ~~(MK)~~ and of the identifier ~~(CID_i)~~ of the defined client device.

[015] (Currently amended) ~~Secure~~ The secure device according to ~~any one of Claims 12 to 14~~ claim 12, ~~characterized in that~~ wherein the means for performing operations of asymmetric cryptography with the aid of the private key ~~(d_i, n_i)~~ determined comprise:

- means of signature ~~(S)~~ of a message ~~(m)~~, and
- means of encipherment ~~(E)~~ of a message ~~(m)~~.

[016] (Currently amended) ~~Secure~~ The secure device according to ~~any one of Claims 14 to 15~~ claim 14, in which the means of determination ~~(4)~~ of the private key comprise furthermore:

- a unit for symmetric encipherment ~~(7)~~, with the aid of the master key ~~(MK)~~, able to encipher the result ~~(ECID$_i$)~~ of a function applied to the identifier ~~(CID$_i$)~~ of the defined client device ~~(C$_i$)~~, and/or
- a unit for calculation ~~(8)~~ of a deterministic algorithm for selecting the second secret part ~~(d$_i$)~~ of the private key on the basis of the result of the encipherment produced by the unit ~~(7)~~ for symmetric encipherment.

[017] (Currently amended) ~~Secure~~ The secure device according to ~~any one of Claims 14 to 16~~ claim 14, ~~characterized in that~~ wherein it furthermore comprises a means of initialization of the client devices of the network, the said means of initialization comprising:

- a means of random generation ~~(2)~~ of a unique master key ~~(MK)~~ and of a plurality of mutually distinct identifiers ~~(CID$_j$, CID$_i$)~~, each identifier being apt to characterize a unique client device ~~(C$_i$)~~ of the client device network,
- a unit for calculation ~~(9)~~ able to select two secret data items ~~(p$_i$, q$_i$)~~ as a function of the value of the second secret part ~~(d$_i$)~~ of the private key and to calculate a first part ~~(n$_i$)~~ of the public key, and
- a unit for calculation ~~(10)~~ of the second part ~~(e$_i$)~~ of the public key, by an Extended Euclid algorithm, on the basis of the secret data ~~(p$_i$, q$_i$)~~, of the second part ~~(d$_i$)~~ of the private key and of the first part ~~(n$_i$)~~ of the public key.

[018] (Currently amended) ~~Computer~~ A division program comprising instructions for the execution of the method steps for enciphering/deciphering a message according to ~~any one of Claims 1 to 11~~ claim 1, when the program

is executed on a secure device embodied on the basis of a programmable calculator.

[019] (Currently amended) ~~Recording~~ A recording medium usable on a secure device embodied on the basis of a programmable calculator on which is recorded the program according to Claim 18.